IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
LYNCHBURG DIVISION

IN THE MATTER OF THE SEARCHES OF **333 PENINSULAR STREET, UNIT B, LYNCHBURG, VA 24501,** **100 REICHARD DRIVE, APT 101 (ALSO KNOWN AS APT. A), MADISON HEIGHTS, VIRGINIA 24572** **TO INCLUDE ALL OUTBUILDINGS, VEHICLES AND THE CURTILAGE SURROUNDING EACH RESIDENCE**	**UNDER SEAL** **Case No.** 6:20mj22

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Daniel Bailey, being first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises, outbuildings, and curtilage of a location known as 333 Peninsular Street, Unit B, Lynchburg, Virginia 24501 ("TARGET ADDRESS #1") located in the City of Lynchburg, Virginia, 100 Reichard Drive, Apt. 101 (also known as Apt. A), Madison Heights, Virginia 24572 ("TARGET ADDRESS #2") located within the County of Amherst, Virginia, (collectively, the "TARGET ADDRESSES") within the Western District of Virginia further described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Administration (DEA) and have been since 2017. I am also a Detective with the Lynchburg Police Department (Virginia) and be been so employed since 2002. I am currently assigned to investigate drug trafficking organizations as a member of the DEA, Washington Field Division/Roanoke Resident Office. My duties as a Task Force Officer involve the investigation of various criminal activities of narcotics traffickers and their associates. In investigating these matters, I have acted as a case agent, an undercover agent, and a contact agent for confidential sources. These investigations have resulted in the issuance of federal search warrants, seizure warrants, indictments, and convictions of persons for federal narcotics violations. During my employment as a law enforcement officer, I have received multiple hours of training in narcotics enforcement and investigative techniques, and I have personally participated in numerous investigations. I have also spoken on numerous occasions with informants, suspects, and other experienced narcotics traffickers concerning the methods and practices of drug traffickers, including the methods and practices used by traffickers of methamphetamine, heroin, and cocaine. I have been involved in the execution of numerous search warrants of physical locations, as well as of electronic devices, including cellphones, and in obtaining location information for those devices.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the TARGET ADDRESSES contain evidence of violations of concealment money laundering, in violation of distribution and possession with intent to

distribute controlled substances, in violation of Title 21, United States Code, Section 841, conspiracy to distribute controlled substances, in violation of Title 21, United States Code, Section 846, and maintaining a drug-involved premises, in violation of Title 21, United States Code, Section 856. There is probable cause to search the locations described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

5. TARGET ADDRESS #1 is a residence located at 333 Peninsular Street, Unit B, Lynchburg, Virginia 24501, located in the City of Lynchburg, Virginia within the Western District of Virginia and described in more detail in Attachment A. TARGET ADDRESS #1 is believed to be a "stash house" or location where narcotics, money, and weapons are stored so that individuals can distribute narcotics.

a. City of Lynchburg government records revealed this dwelling is split into two apartments; A and B. Apartment A is marked as "333 A" on the front door of the dwelling.

b. Surveillance of TARGET ADDRESS #1 revealed that tenants/visitors of Unit A park on Peninsular Street in front of the dwelling. Visitors of Unit B park in a parking area located in the rear of the dwelling.

6. TARGET ADDRESS #2 is a residence located at 100 Reichard Drive, Apt. 101 (also known as Apt. A), Madison Heights, Virginia 24572 located within the County of Amherst, Virginia. TARGET ADDRESS #2 is believed to be the residence of Jerry Carter, Jr.

PROBABLE CAUSE

7. The United States, including the Drug Enforcement Administration (DEA) and the Lynchburg Police Department, are conducting a criminal investigation of Jerry CARTER, Jr.

("CARTER") and others regarding violations of distribution and possession with intent to distribute cocaine and marijuana in violation of 21 U.S.C. § 841(a)(1) and conspiracy to distribute cocaine and marijuana in violation of 21 U.S.C. § 846.

CARTER's Prior Narcotics Activity

8. Per Federal Bureau of Prisons records, CARTER was released from the Federal Bureau of Prisons on or about March 15, 2019 after serving a sentence for Conspiracy to Distribute Cocaine. This affiant knows "TWIN" to be an alias for CARTER. This affiant knows CARTER to have a twin brother.

9. Through the course of this criminal investigation Timothy PAIGE, Joseph BROWN, and Co-Conspirator 1 (CC-1) have been identified as criminal associates of CARTER.

10. Timothy PAIGE is currently pending federal trial in the Western District of Virginia (6:20-cr-7) for his role in a cocaine trafficking conspiracy. PAIGE has been charged with conspiring to and possessing with the intent to distribute cocaine HCL.

11. Joseph BROWN is pending federal trial in the Western District of Virginia (6:20-cr-4) for his role in a cocaine trafficking conspiracy. BROWN has been charged with distributing ounces of cocaine HCL and cocaine base.

12. CC-1 has been identified as the leader of this Drug Trafficking Organization. Based on this investigation, CC-1 is reported to supply CARTER, PAIGE, and BROWN, in addition to others in the Lynchburg area, with distributable amounts of cocaine HCL. This affiant knows CC-1 to have an alias of "Alias 1" and "Alias 2".

13. This affiant identified two cellular phone numbers (434-229-2864 and 434-209-7025) believed to have been previously used by CARTER to further his criminal activity with CC-1 and other co-conspirators, to include but not limited to PAIGE and BROWN. This affiant

served Administrative Subpoenas on SPRINT for subscriber information and toll data records for both of those numbers. The subpoena results have shown that the subscriber for the both of those numbers was "Talisa Mays" with a billing address of "2971 Galts Mill Road, Madison Heights Va 24572."

14. This affiant cross referenced both of those cellular phone numbers through phone downloads of PAIGE and BROWN that had been obtained via previously executed federal and state issued search warrants. This affiant found that both of those numbers were listed under the contact name of "JERRY" and or "TWIN."

15. Based on phone toll analysis this affiant found that one and/or both of those numbers were in contact with multiple numbers that had been previously identified as being used by PAIGE, CC-1, and BROWN. CARTER was also found to be in contact with other identified co-conspirators in this drug trafficking organization (DTO).

16. Based on the data from PAIGE's phone downloads, this affiant also found text messages exchanged between PAIGE and the previously identified numbers of CARTER. Based on this affiant's training and experience, coded text messages were exchanged discussing narcotic transactions. Those messages include, but not limited to, prices of "zips", which is slang for one ounce of cocaine and the availability of "joints", which is known to be slang for one ounce of cocaine or one kilogram of cocaine.

17. Based on the data from BROWN's phone downloads, this affiant also found text messages exchanged between BROWN. This affiant located a text message exchange between BROWN and 434-209-7025 asking if BROWN had anything for "Alias-2" (CC-1).

18. In November 2019, this affiant conducted an interview with Source of Information #1 (SOI-1) who had been arrested for drug trafficking in Lynchburg, Virginia. SOI-

1 advised law enforcement that CARTER was a source of supply for cocaine. SOI-1 advised that he/she knew "Alias-1" to a source of supply for CARTER of cocaine. SOI-1 advised that CARTER would request SOI-1 to travel with CARTER to meet with "Alias-1" in North Carolina to purchase cocaine HCL. SOI-1 advised that he/she would communicate with CARTER via cellular phone. SOI-1 provided this affiant permission to search through SOI-1's cellular phone. This affiant found one of the previously identified numbers stored in the phone under the contact name of "Jerry."

Geolocation Data for CARTER

19. In April of 2020, United States Magistrate Judge Robert Ballou, of the United States Western District of Virginia, approved a search warrant authorizing the collection of geolocation data for a number believed to be used by CARTER, 434-209-7025 (6:20-mj-10).

20. Between April 28, 2020 and April 29, 2020, this affiant monitored the geo-location for 434-209-7025. During that time this affiant observed that phone travel from Charlottesville, Virginia to New York City, New York and back to Nelson County, Virginia.

21. While the vehicle was in New York City, New York, law enforcement officers observed CARTER and another unknown subject place suit cases in the trunk of a vehicle. CARTER then got into the driver seat of that vehicle and drove away. CARTER later travelled back to Virginia that same day.

22. On April 29, 2020, at approximately 10:00 p.m, CARTER was stopped by Virginia State Police Trooper in Nelson County, Virginia. A subsequent search of CARTER's vehicle yield multiple suitcases in the trunk of the vehicle. A search of the car and the suitcases yielded forty-five vacuumed sealed bags containing marijuana (approximate total of forty-five

pounds), a cellular phone, and $19,325 US Currency. CARTER was not charged with any criminal offense at that time and was released from the traffic stop.

23. Shortly after this seizure, this affiant analyzed the toll data of 434-209-7025. Based on that analysis this affiant identified 434-444-3338 as a top contact number. This affiant served an Administrative Subpoena on Sprint for the toll record data and subscriber information for 434-444-3338, This affiant analyzed the results of that subpoena and determined that the subscriber to be "Talisa Mays" with a billing address of "2971 Galts Mill Road, Madison Heights Va 24572."

24. This affiant analyzed the phone toll data of 434-444-3338 leading up to April 29, 2020, date of seizure, and determined that 434-209-7025 was the top contact. This affiant then analyzed the phone toll data of 434-444-3338 for cellular activity post-seizure. This affiant determined that the 434-213-5506 was a top three contact of 434-444-3338. The 434-213-5506 was not located on the phone toll data records of 434-444-3338 prior to the seizure date.

25. On May 7, 2020 this affiant cross referenced the 434-213-5506 through a law enforcement data based that stored phone calls placed by inmates being housed in the Blue Ridge Regional Jail facilities. This affiant located multiple outgoing calls to the 434-213-5506.

26. During a call placed to the number on or about May 2, 2020, the user of 434-213-5506 provided the other party of the call with intimate details of the traffic stop and seizure from April 29, 2020.

27. The DEA obtained a federal warrant (6:20-mj-15) for the location information of cellular phone number, 434-213-5506, on May 11, 2020.

28. On May 20, 2020, according to records obtained from the search warrant for location information from the cell phone, 434-213-5506, traveled from Lynchburg, VA to greater

area of Greensboro, NC. The cell phone, 434-213-5506, was in the area of a mall for a brief period of time before making a return trip towards Lynchburg, Virginia.

29. The location information for cell phone, 434-213-5506, and a possible vehicle description of the vehicle CARTER was presumed to be operating was relayed to the Virginia State Police. Later that same day, a Virginia State Police Trooper stopped that vehicle, which was also was traveling consistent with the location information for cell phone, 434-213-5506, for a traffic infraction in Campbell County, Virginia. CARTER was identified as the driver of the vehicle. A subsequent search of CARTER's vehicle yielded approximately five pounds of marijuana and a cellular phone. CARTER was not charged with any criminal offense at that time and was released from the traffic stop. The cellular phone seized from CARTER on May 20, 2020 was the subject of a search warrant obtained from this Court on June 4, 2020 (6:10-mj-16).

30. Despite law enforcement's seizure of the physical phone from CARTER on May 20, 2020, the DEA began to receive location information again for the cellular phone, 434-213-5506, later that same evening. This affiant continued to conduct surveillance on CARTER and determined that the location of CARTER during those surveillances coincided with incoming geo-location pings.

31. The DEA then obtained additional warrants (6:20-mj-17 and 6:20-mj-19) for the location information from the cellular phone, 434-213-5506. Those warrants have led to the recovery of additional evidence of the ongoing conspiracy to distribute narcotics.

32. During the analysis of the location data, this affiant has determined that the cellular phone, 434-213-5506, had travelled out of the state of Virginia on multiple occasions. Those trips were to the state of North Carolina. Those trips were short in nature before returning back to central Virginia. On June 25 2020, law enforcement officers attempted to conduct visual

surveillance on CARTER as he travelled to/from North Carolina. During the analysis of the location data, this affiant determined that the user had powered off the phone. On two occasions, the user powered the device on for a few moments. Both times the location data revealed the cellular phone was in North Carolina. Surveillances unit were unable to locate CARTER, as he travelled back to central Virginia. Later that same day, this applicant began to receive location data that the cellular phone was in the area of Peninsular Street. This applicant travelled to that location and located a 2015 Cadillac ATS parked at TARGET ADDRESS #1 (back parking area). This applicant then observed CARTER leave that address in the Cadillac ATS and travel to TARGET ADDRESS #2.

33. During the analysis of that data, this affiant has determined that cellular phone, 434-213-5506, has also travelled to Roanoke, Virginia. On June 8, 2020, this affiant was observed meeting with two identified distributors, one of which is suspected to be a Source of Supply (SOS #1) for CARTER.

34. Based on the analysis of all the geo-location data obtained from the warrants described in this affidavit this affiant was able to determine that cellular phone, 434-213-5506, would show in the area of TARGET ADDRESS #2, on an almost nightly basis.

35. Based on that same analysis, this affiant was able to determine that cellular phone, 434-213-5506, would show the area of TARGET ADDRESS #1 on an almost daily basis.

36. Simultaneous physical surveillance of CARTER revealed that CARTER was in the same area of the location data of 434-213-5506.

37. On July 24, 2020, this affiant followed CARTER from Roanoke, VA to TARGET ADDRESS #1. Law Enforcement observed CARTER enter that apartment carrying a bag. Law Enforcement could observe that the shape of the item in that bag was consistent with that of a

compressed kilogram brick off narcotics. Moments after entering the apartment, CARTER was observed leaving with the same bag. However the bag contained significantly less of the substance. It had appeared that the item had be cut in half.

38. On July 30, 2020, this applicant conducted a surveillance on TARGET ADDRESS #1. During that surveillance, this affiant observed CARTER arrive operating a rental vehicle. CARTER exited that vehicle a large duffle bag. That bag contained an item(s) that made the duffle bag sag under the pressure of the weight of the item(s). CARTER collected key from underneath a door mat and used it to unlock TARGET ADDRESS #1. Shortly after CARTER took that bag into the residence, multiple vehicles began to arrive at TARGET ADDRESS #1. The occupants would go into TARGET ADDRESS #1 stay for a matter of minutes and leave. This applicant observed a co-conspirator walk into TARGET ADDRESS #1 with a handful of cash after meeting with a subject in the yard of TARGET ADDRESS #1.

39. In November 2019, this affiant requested any transactional data from the Department of Motor Vehicles (DMV) involving CARTER. This affiant later received certified copies of a DMV application completed by CARTER on March 27, 2019. On that application, CARTER claimed a home address of 101 Reichard Drive, Apt 101, Madison Heights VA 24572 and a phone number of 434-229-2864. TFO Bailey conducted a query of 101 Reichard Drive and found it to be an invalid address. TFO Bailey determined that 100 Reichard Drive, Apartment A (also identified as Apartment “101” per Amherst County Emergency Communications), Madison Heights, VA 24572 is a valid address.

40. This affiant analyzed the data of the contents of this cellular phone, described in paragraph 29 of this affidavit, as authorized by a federal search warrant (6:10-mj-16).

41. During the analysis of that data, CARTER, using coded language, instructed an unidentified Source of Supply to deliver an unknown quantity of an unknown controlled substance to "333 Peninsular Street bottom." During that same text conversation, photographs of marijuana were shared between the two parties.

42. During the analysis of that data, CARTER instructed a Source of Information (SOI-2) to deliver an unspecified quantity of US currency to "100 Reichard Drive 24572". This affiant interviewed SOI-2 in July of 2020. SOI-2 advised this affiant that SOI-2 delivered US currency to 100 Reichard Drive "apartment on the far left" (101 and/or A) for the purpose of paying off a narcotics debt to CC-1. SOI-2 advised he knew CARTER to live at that apartment with a female named "Talisa." SOI-2 advised that they knew CARTER to be a distributor of cocaine HCL and marijuana.

43. During July of 2020, this affiant has spoken with three Confidential Sources of Information (SOI-3, SOI-4, SOI-5) regarding suspicious activity at TARGET ADDRESS #1.

44. SOI-3 advised that for approximately two years SOI-3 had observed an unusually high volume of vehicle traffic going to TARGET ADDRESS #1. SOI-3 advised that most vehicles, including taxi cabs, would come to the apartment for a short period of time (less than five minutes) and leave. SOI-3 specifically identified a dark colored Cadillac car that would go to and from the residence multiple times a day.

45. SOI-4 advised that for an extended period of time SOI-4 had observed an unusually high volume of vehicle traffic going to TARGET ADDRESS #1. SOI-4 advised that most vehicles would come to the apartment for a short period of time and leave.

46. SOI-5 advised that for over, approximately, two years SOI-5 had observed an unusually high volume of vehicle traffic going to TARGET ADDRESS #1. SOI-5 advised that

they did not believe anyone lived that in that apartment and that it was used to strictly sell narcotics. SOI-5 advised that they had observed individuals go into TARGET ADDRESS #1, carrying quantities of U.S. currency.

47. On July 17, 2020 this affiant conducted a surveillance on TARGET ADDRESS #1. During that surveillance, this affiant observed a Co-Conspirator (CC #2) walking from the TARGET ADDRESS carrying an unknown item in their hand. CC #2 then stood at the top end of the driveway. While standing there, it appeared to this affiant, that CC #2 was attempting to hide the item that CC #2 was holding in their hand behind their leg. CC #2 was also looking around as if to see if anyone was watching CC #2. A few minutes later, this affiant observed a vehicle pulling up alongside where CC #2 was standing. This affiant observed CC #2 drop the item CC #2 was holding onto the lap of the driver of the vehicle. This affiant then followed that vehicle into Amherst County, Virginia before losing sight of this vehicle in the area of the address of the registered owner of the vehicle. A few moments passed, approximately ten minutes, before this affiant observed the vehicle coming from the direction of that address. Law enforcement conducted a traffic stop on that vehicle for traffic violation. During the course of that traffic stop, a narcotic detection K-9 conducted a free air sniff around the exterior of that vehicle and alerted to the odor of narcotics coming from the vehicle. A search of that vehicle was conducted but no illegal substance was located.

48. On August 12, 2020, law enforcement was conducting a surveillance at TARGET ADDRESS #1. During that course of that surveillance, law enforcement observed CARTER and multiple other co-conspirators enter TARGET ADDRESS #1. Later, during that same period of surveillance, law enforcement observed Quaindrick WILLIAMS walk into TARGET ADDRESS #1. WILLIAMS was in TARGET ADDRESS #1 for a period of not more than five minutes.

When WILLIAMS walked out of TARGET ADDRESS #1, law enforcement observed a large item in a pant pocket of WILLIAMS. It should be noted that WILLIAMS was carrying a cellular phone in his hand. WILLIAMS then left in a motor vehicle. Law enforcement conducted a lawful traffic stop on that vehicle shortly after leaving TARGET ADDRESS #1. During the traffic stop, law enforcement searched the vehicle. WILLIAMS was found in possession of over one hundred grams of suspected marijuana. WILLIAMS was released without being charged at that time. Shortly after that traffic stop, CARTER and the other co-conspirators left TARGET ADDRESS #1, in separate vehicles, at a high rate of speed. Two of those vehicles were found to be rental vehicles.

49. This affiant conducted a query through the Virginia Employment Commission and determined that CARTER has not had legitimate employment since his release from federal prison.

50. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that Jerry CARTER, Jr has violated Title 21, United States Code, Section 841, to wit: distribution of cocaine and marijuana, which are controlled substances, and that drugs, documentation, and other items related to the illegal distribution of cocaine and marijuana will be located in the residences at TARGET ADDRESS #1 and TARGET ADDRESS #2.

51. Based upon my training, expertise, and experience, I know that:

a. Distributors of controlled substances and money launderers often keep ledger books, telephone books, receipts, drug/money customer lists, photographs and other papers that identify co-conspirators and their locations or residences and that relate to the importation, transportation, purchasing and distribution of

controlled substances and proceeds derived from said sales;

b. Drug traffickers generate substantial profits because of drug dealing which the courts have recognized as probative evidence of crimes motivated by greed, in particular, trafficking controlled substances. Drug traffickers often place assets in corporate entities in order to avoid detection of those assets by law enforcement agencies. These assets often are placed in other person's names, even though the drug dealers continue to use these assets and exercise dominion and control over them. They also often maintain on hand large amounts of United States currency in order to operate and finance their ongoing drug business;

c. Drug traffickers commonly "front" (i.e. provide on consignment) controlled substances to their clients and the aforementioned books, records, receipts, notes, ledgers, etc. are maintained where the drug traffickers have ready access to them. It is common practice for large-scale drug dealers to conceal contraband, proceeds and drug sales and records of drug transactions in secure locations within their residences, stash houses, and/or places of business for ready access and to conceal such items from law enforcement authorities. Persons involved in large scale drug trafficking often conceal in their residences, stash houses, and/or places of business, caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry, automobile titles and other items of value which are proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting or spending large sums of money acquired from engaging in narcotics trafficking activities;

d. When drug traffickers amass large proceeds from the sale of drugs, they often

attempt to legitimize or "launder" these profits. To accomplish this, drug traffickers may utilize, but are not limited to, domestic and foreign banks and/or financial institutions and their attendant services, such as securities, cashier's checks and money drafts;

e. It is common practice for large-scale drug traffickers to travel to their source and distribution points to facilitate their trafficking. After purchasing their drugs, drug traffickers often transport or cause to be transported their drugs to areas in which they will distribute them. The methods of transportation include, but are not limited to, commercial carriers, private airplanes, ocean going motor vessels, rental or private automobiles, and government or contract mail carriers;

f. Drug traffickers commonly cause to be taken photographs of themselves, their associates, their property and items used in the distribution of controlled substances. These traffickers usually maintain these photographs at their residences or places of business;

g. Narcotics traffickers use safes, surreptitious compartments and money counting machines to count and store the profits of their narcotics business;

h. Narcotics traffickers commonly possess at their residences, stash houses, or places of business, drugs, paraphernalia, and materials for packaging, cutting, weighing and distributing heroin, including, but not limited to scales, plastic wrap, plastic baggies, paper slips, tin foil, stamp pads, stamp ink and various cutting agents;

i. Drug traffickers commonly use electronic devices and storage components including, but not limited to, cellular telephones, computers, telex machines,

facsimile machines, currency counting machines, telephone answering machines, computer software, tapes, discs, CD, DVDs, and audio tapes to store records of drug sales, ledgers, supplier's/customer's contact information, financial records, images, audio/video recordings and other related documents related to the trafficking and sale of narcotics;

52. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that U.S. Currency, documentation, and/or other items related to the illegal distribution of narcotics and money laundering further described in Attachment B will be located at the TARGET ADDRESSES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

53. As described above and in Attachment B, this application seeks permission to search for records that might be found at the TARGET ADDRESSES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

54. *Probable cause.* I submit that if a computer or storage medium is found at the TARGET ADDRESSES, there is probable cause to believe relevant records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

55. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the Crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the

TARGET ADDRESSES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the Criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the Crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant

insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a Crime (e.g., internet searches indicating Criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to communicate online with a victim in a fraud scheme, the individual's computer will generally serve both as an instrumentality for committing the Crime, and also as a storage medium for evidence of the Crime. The computer is an instrumentality of the Crime because it is used as a means of committing the Criminal offense. The computer is also likely to be a storage medium for evidence of Crime. From my training and experience, I believe that a computer used to commit a Crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the Criminal conduct was achieved; records of Internet discussions about the Crime; and other records that indicate the nature of the offense.

56. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

57. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

58. In my training and experience, it is likely that the TARGET ADDRESSES will contain at least one Apple brand device, such as an iPhone or iPad, because CARTER was previously found in possession of an Apple iPhone and the search of that phone revealed messages sent as iMessages.

59. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

60. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

61. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1)

the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

62. The passcode or password that would unlock the Apple device(s) found during the search of the TARGET ADDRESSES is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the Apple device(s) found during the search of the TARGET ADDRESSES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

63. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the TARGET ADDRESSES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the TARGET ADDRESSES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

64. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the TARGET ADDRESSES as described

above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

65. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the TARGET ADDRESSES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the TARGET ADDRESSES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

66. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A, in order to seek the items described in Attachment B.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Daniel Bailey
Daniel Bailey, Task Force Officer
Drug Enforcement Administration

Received by reliable electronic means and sworn and attested to by telephone on this 12th day of August 2020.

Robert S. Ballou
ROBERT S. BALLOU
UNITED STATES MAGISTRATE JUDGE